



Department of Homeland Security Daily Open Source Infrastructure Report for 23 August 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- Reuters reports border police say that illegal immigrants and drug traffickers are now using dilapidated bicycles to make a swift, night time dash over the desert to Arizona from Mexico. (See item [20](#))
- The Boston Herald reports that according to a new report, emergency responders to a terror attack on Massachusetts Bay Transportation Authority subway tunnels would be crippled by radios muffled by static and cut off from incident commanders. (See item [32](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *August 22, Times-Herald (CA)* — **Wires damaged in thwarted robbery.** Copper wires from a Pacific Gas & Electric (PG&E) substation near the Valero refinery near Benecia, CA, were destroyed early last week in an apparent unsuccessful theft attempt. PG&E spokesperson David Eisenhower said someone broke into the substation, took temporary copper ground cables, cut them up, and put the wires in nearby bushes. It's unknown how many copper wires were cut up. Typically, in such theft instances, whoever broke into the substation would return to the area later and pick up the copper wire in an easily accessible spot, Eisenhower said. It's unknown when the attempted theft actually occurred, Eisenhower said.

Source: http://timesheraldonline.com/ci_4218723

2. *August 21, WLBZ-2 (ME)* — **Vandals blamed for Freeport power failure.** A power outage at a mall in Freeport, ME, Sunday, August 20, was likely caused by vandalism, according to Central Maine Power (CMP). CMP spokesperson John Carroll says someone using a gun damaged ceramic insulators on high-voltage lines between Yarmouth and Freeport. He says rain seeped into the insulators, causing the failure. The damage knocked out electricity in parts of Freeport, Yarmouth, Durham, and Brunswick. The lights went out at 2:20 EST Sunday afternoon.

Source: <http://www.wlbz2.com/news/article.aspx?storyid=40362>

3. *August 21, Christian Science Monitor* — **Canada seeks Niagara Falls power.** Niagara Falls produces more hydroelectric power than any other waterfall in the world. Ontario, Canada's government is looking at the falls as an alternative power source as the government struggles to make sure it has enough electricity. Ontario has also vowed to shut down the province's coal-burning power plants. Now, the second-largest tunneling project ever will bring more water to existing turbines on the Canadian side, generating enough new electricity to run 160,000 homes. Construction will begin in early September; scheduled completion is in 2009. The tunnel will take 17,500 cubic feet of water per second from the Niagara River above the falls to the Sir Adam Beck generating station. "We are in effect adding more fuel by adding more water, making sure the existing turbines run at top capacity," says Emad Elsayed of Ontario Power Generation. The falls on the U.S. side produce even more hydroelectric power than the Canadian side. All that water diversion means there is less water flowing over the falls. Hydroelectric projects on both the American and the Canadian sides divert 50 percent to 75 percent of the water in the Niagara River into tunnels to run turbines.

Source: <http://www.cbsnews.com/stories/2006/08/21/tech/main1916244.s.html>

4. *August 19, New York Times* — **BP twice avoided Prudhoe pipeline being smashed or broken open.** Twice late last week, a major pipeline in the hobbled Prudhoe Bay oil field came close to being smashed or broken open — once when a drilling rig nearly tipped over onto it, and again when a sudden surge inside the line caused it to twitch like a live wire, knocking the elevated pipe off its support mounts and onto the tundra below. In the end, the pipeline stayed intact, no oil leaked, and no one was hurt, BP spokesperson Daren Beaudou said. The pipeline involved in the two near misses carries a mixture of crude oil, natural gas, and water out of the Point McIntyre field, north of Prudhoe, to a western Prudhoe separation plant. The western side of Prudhoe is producing oil while the eastern half remains idle because of corroded pipelines.

Source: http://www.mywesttexas.com/site/news.cfm?newsid=17085990&BRD=2288&PAG=461&dept_id=474107&rfti=6

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

5. *August 22, Cape Cod Times (MA)* — **Homes evacuated after gas line split.** Monday, August 21, a Department of Public Works backhoe hit a natural gas service line in South Dennis, MA, and ripped it from the main line on Uncle Bob's Way near the intersection of Dorothy Way.

Firefighters and police officers blocked off surrounding roadways and evacuated 15 nearby homes as a result.

Source: <http://www.capecodonline.com/cctimes/homesevacuated22.htm>

6. *August 22, WIS 10 (SC)* — **Unknown chemical spill in South Carolina prompts shelter-in-place.** Crews responded to reports of a possible chemical spill in Cayce, SC, Tuesday morning, August 22. Officials say a garbage truck was in the area, and authorities believe some kind of container containing an unknown substance was compacted in the back of that truck, causing it to rupture. One of the workers on the truck was overcome by fumes. Police and fire personnel surrounded the neighborhood, cordoned off a large portion of it, told people to stay inside and turn off their air conditions.

Source: <http://www.wistv.com/Global/story.asp?S=5311230>

7. *August 22, WPEC News 12 (FL)* — **Chlorine leak forces residents to remain indoors.** A chlorine leak occurred at a water treatment plant Riviera Beach, FL, during routine maintenance. As a result, officials went door to door and asked people to stay inside.

Source: <http://www.news12now.com/engine.pl?station=wpec&id=3798705&template=breakoutnews.shtml>

[[Return to top](#)]

Defense Industrial Base Sector

8. *September 01, National Defense* — **Defense engineers ponder "modest adjustments" for connecting forces.** Incompatible weapon systems and disjointed information networks continue to be a source of frustration at the Department of Defense (DoD), which launched an ambitious campaign six years ago to reshape the military services into “network-centric” forces. While the services have acquired an abundance of network-based technologies in recent years for the war in Iraq, most of the systems they still operate were developed and purchased a decade or two ago, in isolation from each other. These “legacy” technologies, for the most part, cannot exchange or share data. The Pentagon leadership has acknowledged that it is not going to replace current technologies in the near future, and that “modest investments” can be made to improve existing hardware, said John J. Young Jr., director of defense research and engineering. Young's team will deliver a near-term roadmap — for no later than 2010 — of “what things we can do with the tools we have to get the maximum amount of network centric force capability,” Young said. The team also will outline a longer-term blueprint, for 2015 and beyond. This plan would offer hypothetical scenarios for networking systems if the next-generation technologies become available.

Source: <http://www.nationaldefensemagazine.org/issues/2006/September/DefenseEngineers.htm>

[[Return to top](#)]

Banking and Finance Sector

9.

August 22, VNUNet — **Volume of "romantic" spam jumps sharply.** Security experts Tuesday, August 22, reported a "sharp increase" in the amount of spam email offering "romantic" contacts. Sophos warned that such e-mails can have a number of aims, including confirming that an e-mail address is active and thus more attractive to spammers. Also, such spam can lead to a confidence trick that sees the recipient build up a relationship with their new electronic friend and ultimately hand over money or personal information.

Source: <http://www.vnunet.com/vnunet/news/2162747/volume-romantic-sp-am-jumps>

10. *August 21, Websense Security Labs* — **Phishing Alert: GE Money Savings.** Websense Security Labs has received reports of a new phishing attack that targets customers of GE Money Savings. Users receive a spoofed e-mail message claiming that, following a notification from Visa, they are investigating some Visa card and Check card accounts that might be compromised. The e-mail requests users to validate account information, and provides a link to a fake site that attempts to collect login information as well as account and card information, such as ATM pin number, card number, and user ID.

Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=581>

11. *August 21, Computerworld* — **Stanford University's Password Hash.** Professors and students at Stanford University have developed a plug-in tool for Web browsers called Password Hash (PwdHash) to prevent phishing. "Internet users often use the same password at many Websites," says Dan Boneh, an associate professor at Stanford. "A phishing attack on one site will expose their passwords at many other sites." By simply adding "@@" to the beginning of a password when registering on a Website, PwdHash combines the user's password with the site's domain name in an algorithm that customizes a password for the user. If a password is stolen from a malicious site, it won't work on the authentic site "although you typed in the same password," explains professor John Mitchell. Although the idea of adding a cryptographic hash function to a password isn't new, Mitchell and his team have advanced the technology by making it easy enough for end users to apply. The software is available for free, with versions for the Internet Explorer and Firefox browsers. Mitchell is trying to persuade major browser vendors to include PwdHash in upcoming releases.

Source: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9002549&taxonomyId=17>

12. *August 20, Montreal Gazette (Canada)* — **New York bank executive pleads guilty to Montreal-based telemarketing scam.** A former vice-president of a New York bank has pleaded guilty to his role in a \$30 million U.S. telemarketing scheme that originated out of Montreal. Raymond Payne was arrested in New York in January 2005, just days before the Canadian police arrested 28 other people, including the two alleged ringleaders. The telemarketing ring is alleged to have bilked money out of 100,000 victims, mostly low-income earners in the U.S. who had credit problems. Telemarketers convinced victims they would be sent credit cards if they paid a fee that ranged between \$249 and \$299. Instead of a credit card the victims received manuals on how to repair their bad credit. Payne was a vice-president with the HSBC Bank, working out of its corporate offices in Manhattan. He managed an account held by a Montreal company named First Choice Tele-Services Corporation. The account was used to collect fees victims paid to First Choice through electronic transfers.

Source: <http://www.canada.com/montrealgazette/news/story.html?id=f16aff08-3399-46ec-96d7-74fe6becf773&k=98386>

13. *August 18, Websense Security Labs* — **Phishing Alert: Evergreen Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Evergreen Credit Union, which is based in Maine. Users receive a spoofed e-mail message claiming that their account has been accessed from a foreign IP address and that this activity must be verified. The URL provided in the e-mail is a phishing site that attempts to collect users' account information.
Source: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=579>

[\[Return to top\]](#)

Transportation and Border Security Sector

14. *August 22, American City Business Journals* — **Northwest Airlines to lay off 38, outsource ground operations.** Northwest Airlines will outsource its ground operations at Louisville International Airport and 67 other airports. The move, which was agreed to earlier this year by the International Association of Machinists, will result in the elimination of 35 full-time and three part-time positions at Louisville International, said Roman Blahoski, spokesperson for Eagan, MN-based Northwest Airlines. St. Louis-based Airport Terminal Services will take over the work in January, Blahoski said. The displaced workers — baggage handlers, ticket agents, and gate agents — will be given the opportunity to retire, apply for a position with Airport Terminal Services, or transfer to another airport where Northwest will continue to maintain its ground operations, Blahoski said.
Source: <http://biz.yahoo.com/bizj/060818/1333953.html?.v=1>
15. *August 22, BBC* — **Russian plane crashes in Ukraine.** A Russian plane crashed in eastern Ukraine minutes after sending a distress signal, killing all 170 people on board, officials said. The Tupolev-154 was flying from the Russian Black Sea holiday resort of Anapa to St Petersburg when it disappeared from radar screens. Emergency workers were at the scene of the burning wreckage, about 45km (30 miles) north of the city of Donetsk. The crew of the Pulkovo Airlines flight sent a distress signal at 1537 Moscow time (1137 GMT), and the plane disappeared from radar screens two minutes later, Russian officials said. The fuselage of the plane was entirely destroyed and a thick pall of white smoke hung in the air, an Agence France-Presse journalist reported from the scene. Reports of the cause of the crash were confused. Ukraine's emergencies ministry said a fire had broken out on board, while Russian officials said the accident was probably caused by severe air turbulence. St Petersburg-based Pulkovo Airlines is one of Russia's larger carriers. The crash is the third serious air disaster in the region this year.
Source: <http://news.bbc.co.uk/1/hi/world/europe/5274958.stm>
16. *August 22, Cox News Service* — **Amtrak brings out old rail cars as part of standby evacuation plans.** Under a \$700,000 contract, Amtrak has refurbished 24 mothballed rail cars and brought them to the New Orleans train station, where they are now on standby for the current storm season, said Brian Turmail, a spokesperson for the Department of Transportation (DOT). The arrangements are part of an evacuation program financed by the Federal Emergency Management Agency. Turmail said that if a hurricane threatens, the 24 restored cars plus 23 more cars now used for Amtrak's regular passenger service in the region would be

mobilized for the effort, he said. A single train can take as many as 1,600 passengers out of the danger zone.

Source: http://www.oxfordpress.com/hp/content/shared/news/stories/FE_MA_AMTRAK22_COX_W4918.html

17. *August 22, Associated Press* — Runway resurfacing could cause weekend delays at Logan.

Boston's Logan International Airport plans to close one of its four main jet runways for resurfacing on weekends through October, which could mean delays for travelers. Resurfacing work on the same 10,005-foot runway last summer created numerous travel delays, but work was done on both weekdays and weekends, depending on favorable weather conditions for construction work. This time, closings will happen only on weekends. The runway closings begin this weekend, lasting from 10 p.m. Friday through 6 a.m. EDT Monday each weekend through October 25, according to the Massachusetts Port Authority, which operates the airport. Late this year, Massport expects to open a new 5,000-foot runway on the south side of the airport that officials expect will help reduce delays.

Source: http://www.usatoday.com/travel/flights/2006-08-22-boston-delays_x.htm

18. *August 22, Associated Press* — Fumes at Minneapolis-St. Paul airport send 12 to hospital.

A security checkpoint was closed at the Minneapolis-St. Paul International Airport on Tuesday, August 22, after security officials complained of irritating fumes. Airport spokesperson Pat Hogan said that at about 11 a.m. CDT security screeners complained about an odd smell that was irritating their eyes, noses and throats. Twelve employees of either airlines or the Transportation Security Administration were taken to area hospitals. All were lucid, conscious and breathing when they left, Hogan said. He said some of screeners described the odor as sweet, like perfume, with others said it was peppery. He speculated the fumes could have come from something a traveler threw into a trash bin while in the security line. The incident happened hours before President George Bush was scheduled to arrive at 2 p.m. at a National Guard base adjacent to the airport.

Source: <http://www.duluthsuperior.com/mld/duluthsuperior/news/politics/15333768.htm>

19. *August 22, BBC* — Plane note prompts airport alert. A flight from Britain's Luton Airport to Majorca was delayed as police inspected an aircraft after cabin crew found a "scribbled note" on board. The note was found on the back of a safety card as cabin crew prepared the plane for take-off. The aircraft was cordoned off as police went on board to inspect the plane. The scare comes during a heightened state of alert at UK airports following an alleged bomb plot to blow up several transatlantic airliners. On Friday, a charter flight from London to Egypt was diverted for security checks after a note claiming there was a bomb on the plane was found scribbled on a sick bag.

Source: http://news.bbc.co.uk/2/hi/uk_news/england/5275358.stm

20. *August 21, Reuters* — Mexico migrants use cycles to cross Arizona desert. Illegal immigrants and drug traffickers are using dilapidated bicycles to make a swift, night time dash over the desert to Arizona from Mexico, border police say. Border Patrol agents in the desert state are finding dozens of the bikes dumped at hamlets such as Three Points, southwest of Tucson, which are used as staging areas by smugglers ferrying marijuana and immigrants on to cities inland. "The illegals use bicycles, either riding them on ranch roads or the foot trails, as a quicker means of getting north," said Border Patrol agent Kevin Nutwell as he inspected a rusty

bike discarded on one lonely trail south of Three Points. Agents say it takes up to three days to walk the 45-mile trail from the border to Three Points, where immigrants are picked up for an onward journey to Tucson and Phoenix either by truck or packed into cars. Stealthy cyclists who make the trip in groups of up to 10 people led by a guide or "coyote" can make the trip in just a few hours.

Source: http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyid=2006-08-22T003104Z_01_N21200756_RTRUKOC_0_US-LI-FE-USA-BICYCLES.xml&src=rss&rpc=22

[[Return to top](#)]

Postal and Shipping Sector

21. *August 17, Reed Business Information* — FedEx launches Critical Inventory Logistics.

FedEx recently launched its new Critical Inventory Logistics service focusing on high value and time critical inventory for shippers in telecommunication, semiconductor, biomedical and other high technology industries. "Customers are increasingly looking to FedEx for our expertise in managing just-in-time, critical inventories," said Tom Schmitt, president and CEO of FedEx Global Supply Chain Services. FedEx Critical Inventory Logistics personnel will help customers determine how to best position their critical inventories throughout the FedEx network and develop plans to optimize their supply chains.

Source: <http://www.purchasing.com/article/CA6361146.html?industryid=2150>

[[Return to top](#)]

Agriculture Sector

22. *August 21, Stop Soybean Rust News* — Soybean rust found in South Carolina. Asian soybean rust has been found in sentinel-plot soybeans in Calhoun, SC. This is the first rust in the state this year and the farthest north rust has been found in the U.S. in 2006. There are now 35 counties in seven states that have had rust in 2006.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=924>

23. *August 21, Agence France-Presse* — Germany reports first bluetongue cases on cattle, sheep farms. Germany has reported its first cases of sheep virus, also known as bluetongue, at nine farms in the western state of North Rhine-Westphalia. The federal agriculture ministry said the virus had been confirmed at eight cattle farms and one sheep farm, all near the city of Aachen on the Belgian border. The Netherlands and Belgium reported fresh cases Monday, August 21, after an outbreak last week. The viral infection affects sheep almost exclusively but it can be found in other ruminants.

Bluetongue information: <http://www.fao.org/AG/AGAINFO/subjects/en/health/diseases-cards/bluetongue.html>

Source: http://news.yahoo.com/s/afp/20060821/hl_afp_germanfarmhealth_sheep_060821160857

[[Return to top](#)]

Food Sector

24. *August 21, Agence France–Presse* — **Court declines to lift ban on Coke, Pepsi in Indian state.** A court in southern India denied a plea to lift a state ban on beverages sold by Coca-Cola and PepsiCo pending an appeal by the manufacturers against the order. The two companies had asked for a reprieve from the ban imposed this month by the communist-ruled southern state of Kerala. But the court decided it would not issue a temporary waiver of the ban as requested and wanted to hear the case in full, a court official said. Kerala state officials slapped the ban on sale and manufacturing of the drinks after claims by an environmental group that the products contained high levels of pesticides.

Source: http://news.yahoo.com/s/afp/20060821/hl_afp/indiacourtcompanycokepepsi_060821100932

25. *August 19, San Diego Union–Tribune* — **Oysters suspected after twelve became ill.** The San Diego, CA, Health and Human Services Agency has received reports of people possibly sickened by eating raw oysters, and it is urging precautions. Twelve people have been infected with vibrio parahaemolyticus, a bacterium common to oysters. The cases were reported from June 1 through Thursday, August 17. Nine people said they had eaten raw oysters in Mexico or the U.S. shortly before becoming ill. Symptoms can include abdominal cramping, nausea, diarrhea, fever and chills.

Source: <http://www.signonsandiego.com/news/metro/20060819-9999-7m19oyster.html>

[[Return to top](#)]

Water Sector

26. *August 21, Financial Times* — **Water scarcity affects one in three.** A third of the world's population is suffering from a shortage of water, raising the prospect of "water crises" in countries such as China, India and the U.S. Scientists had forecast in 2000 that one in three would face water shortages by 2025, but water experts have found that this threshold has already been crossed. About a quarter of the world's population lives in areas of physical water shortage, where natural forces, over-use and poor agricultural practices have led to falling groundwater levels and rivers drying up. A further one billion people face economic water shortages, because lack the necessary infrastructure. The findings come from a report compiled by 700 experts over five years, the Comprehensive Assessment of Water Management in Agriculture from the International Water Management Institute, presented on Monday, August 21, at World Water Week in Sweden, an international meeting of water experts. Shortages of water are already happening. Egypt imports more than half of its food because it lacks enough water to grow more. In Australia, there is a water shortage in the Murray–Darling basin. In the U.S., there are increasing disputes with Mexico over the sinking levels of water in the Colorado river.

Source: <http://www.ft.com/cms/s/3e3eeab2-3137-11db-b953-0000779e2340.html>

27. *August 18, KATV (LA)* — **Some sections of New Orleans still without drinking water.** The most-devastated section of New Orleans's Lower Ninth Ward, an area that was torn apart by Hurricane Katrina and floodwaters, is still without drinking water nearly a year after the storm.

Following a meeting between residents and the New Orleans Sewerage and Water Board on Thursday, August 17, community activists said there is no indication of when the problem will be solved. Because of the extreme devastation in the area, crews have been unable to open major valves that would move water and reveal pipe leaks, said Tommie Vassel, the board's president pro tempore. Repairs also have been slow because it took weeks to pump the area dry after Katrina on August 29, 2005 and again after Hurricane Rita on September 24, 2005, Vassel said.

Source: <http://www.katc.com/Global/story.asp?S=5298257>

[[Return to top](#)]

Public Health Sector

28. *August 22, Agence France–Presse* — **Japan and China join forces to combat bird flu.** Japan and China have joined forces to study bird flu and other infectious diseases through an exchange of researchers. The heads of Japan's National Institute of Infectious Diseases and the Chinese Center for Disease Control and Prevention signed an agreement to jointly study infectious diseases and cooperate in finding vaccines. Japan signed a similar agreement in April with South Korea, opening the way for cooperation among the three countries in research and personnel exchanges. "Joint research with Japan will play an important role in detecting an early bird flu outbreak," said Yang Weizhong, the head of the Chinese organization. The disease has killed about 140 people, mostly in Asia including 14 in China, since 2003. Japan has reported infections in birds but no human deaths from avian influenza.

Source: http://news.yahoo.com/s/afp/20060822/hl_afp/healthjapanchina_diseasefluscience_060822094841

29. *August 21, Xinhua (China)* — **New Hand, Foot and Mouth Disease cases occur in Malaysia.** Sarawak state in eastern Malaysia has detected 23 new cases of Hand, Foot and Mouth Disease (HFMD) in the past 24 hours, an official said Sunday, August 20. Among the new cases reported, 10 children have been hospitalized, said State Deputy Chief Minister George Chan. Six of the children were admitted to the Miri hospital, two in Bintulu and the rest in Sibu and Limbang, said Chan. The latest figure brought the total number of children infected since the disease broke out early this year to 13,800. So far, the disease has claimed 13 lives.

HFMD information: <http://www.cdc.gov/ncidod/dvrd/revb/enterovirus/hfhf.htm>

Source: http://english.people.com.cn/200608/21/eng20060821_295187.ht ml

30. *August 20, Lancet* — **Counterfeit anti-infective drugs.** The production of counterfeit or substandard anti-infective drugs is a widespread and under-recognized problem that contributes to morbidity, mortality, and drug resistance, and leads to spurious reporting of resistance and toxicity and loss of confidence in health-care systems. Counterfeit drugs particularly affect the most disadvantaged people in poor countries. Although advances in forensic chemical analysis and simple field tests will enhance drug quality monitoring, improved access to inexpensive genuine medicines, support of drug regulatory authorities, more open reporting, vigorous law enforcement, and more international cooperation with determined political leadership will be essential to counter this threat.

Source: http://www.thelancet.com/journals/laninf/article/PIIS1473309_906705813/fulltext

31. *August 15, Emerging Infectious Diseases* — **State plans for containment of pandemic influenza.** A review to assess differences and similarities of the states in planning for pandemic influenza was made. Researchers reviewed the recently posted plans of 49 states for vaccination, early epidemic surveillance and detection, and intraepidemic plans for containment of pandemic influenza. All states generally follow vaccination priorities set by the Advisory Committee on Immunization Practices. They all also depend on National Sentinel Physician Surveillance and other passive surveillance systems to alert them to incipient epidemic influenza, but these systems may not detect local epidemics until they are well established. Because of a lack of epidemiologic data, few states explicitly discuss implementing nonpharmaceutical community interventions: voluntary self-isolation (17 states [35 percent]), school or other institutional closing (18 [37 percent]), institutional or household quarantine (15 [31 percent]), or contact vaccination or chemoprophylaxis (12 [25 percent]). The review indicated the need for central planning for pandemic influenza and for epidemiologic studies regarding containment strategies in the community.

Source: http://www.cdc.gov/ncidod/EID/vol12no09/06-0369.htm?s_cid=ei_d06_0369_x.

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

32. *August 22, Boston Herald* — **Report: Massachusetts emergency responders would have limited communications during a subway attack.** Emergency responders to a terror attack on Massachusetts Bay Transportation Authority (MBTA) subway tunnels would be crippled by radios muffled by static and cut off from incident commanders as they faced murky chaos beneath the ground, according to a new report. A review by a key legislative committee has found that communication between police, fire and emergency management service officials remains dangerously fragmented, with agencies unable to talk instantly underground. The Legislature's Public Safety Committee is expected to release a report within the next few weeks that details shortcomings in the state's ability to respond to mass transit attacks. MBTA officials say they are already in the midst of an unprecedented effort to upgrade emergency communications. During the next 18 months, MBTA will install new digital equipment that will allow instantaneous communication between police and fire officials across the region.

Source: <http://news.bostonherald.com/localRegional/view.bg?articleid=153877>

33. *August 22, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: At 5:00 a.m. EDT Tuesday, August 22, Tropical Depression (TD) Four was located about 140 miles south of the Cape Verde Islands with sustained wind speeds near 35 mph. TD Four remains a large and well organized system and is likely to become the fourth named storm of the season during the next 24 hours — Debby. Eastern Pacific: At 5:00 a.m. EDT Tuesday, the newly-formed Tropical Storm Ileana with winds about 52 mph was located near 14.0 north

105.6 west southwest of Acapulco, Mexico. Ileana is expected to intensify during the next 24 hours. At 5:00 a.m. EDT Tuesday, Tropical Storm Hector with winds about 40 mph was located about 1,200 miles east of the Hawaiian Islands where the system continues to deteriorate. At 5:00 a.m. EDT Tuesday, Hurricane 01C Ioke was located near 14.9 north 168.1 west or about 155 miles southeast of Johnston Island and about 800 miles west–southwest of Honolulu Hawaii. The storm, with sustained winds about 135 mph, is expected to move toward the northwest near 13 mph and this motion is expected to continue for the next 24 hours.

To view other Situation Updates: <http://www.fema.gov/emergency/reports/index.shtm>

Source: <http://www.fema.gov/emergency/reports/2006/nat082206.shtm>

34. *August 21, Washington Technology* — **Mobile units can help speed response during catastrophes.** To cope with an emergency, key government organizations, such as police, first responders and human services agencies, must be better able to communicate with each other, and they must have quick access to critical data. To meet these needs, many states are considering mobile disaster recovery equipment and solutions. The model for data recovery in a disaster has been to pay for use of a private data center. Many large IT and telecommunications companies have such operations, and many private sector businesses use them. State agencies looking to recover just 35 seats are paying \$11,500 per month, plus fees ranging up to \$10,000 to declare a disaster, plus additional usage fees after 30 days, all for the right to use a backup data center within 48 hours of an emergency. Those prices may be within range for major corporations, but not for state and local government agencies, said Louisiana CIO Rizwan Ahmed. The business model of mobile disaster recovery solution providers offers cheaper service, said Ahmed, who is working on a deal with several mobile disaster recovery companies for services to state agencies under one contract, he said.

Source: http://www.washingtontechnology.com/news/21_16/homeland/29153-1.html

35. *August 03, National Council on Disability* — **NCD releases report on impact of hurricanes Katrina and Rita.** The National Council on Disability (NCD) recently released a report focusing on the effects of hurricanes Katrina and Rita on people with disabilities. This report demonstrates that people with disabilities were disproportionately affected by the hurricanes because their needs were often overlooked or completely disregarded. Their evacuation, shelter, and recovery experiences differed vastly from the experiences of people without disabilities. People with disabilities were often unable to evacuate because transportation was inaccessible. Moreover, people with visual and hearing disabilities were unable to obtain necessary information pertinent to their safety because said communication did not comply with federal law. NCD offers these findings to guide the President, Congress, and other emergency planners to develop inclusive emergency preparedness and response plans. See source for full text report.

Source: http://www.ncd.gov/newsroom/publications/2006/pdf/hurricanes_impact.pdf

[[Return to top](#)]

Information Technology and Telecommunications Sector

36. *August 22, Sophos* — **Spoof e-mail from anti-child porn agency carries Trojan horse.** Sophos has warned of a Trojan horse that has been spammed out in an e-mail claiming to come from an organization fighting child pornography on the Web. The e-mails claim that the recipient's e-mail address has been found in a child porn database discovered by the

Association of Sites Advocating Child Protection, but really contains a Trojan horse. The Troj/Agent-CPK Trojan horse has been spammed out in the e-mail messages, with the subject line "CP investigation was started." Attached to the e-mail is a file called asset576.zip, which unzips to a file called asset.txt.exe. Running the executable file installs the Trojan horse onto the user's computer.

Source: http://www.sophos.com/pressoffice/news/articles/2006/08/troj_an-agent-cpk.html

37. *August 21, Security Focus* — **Multiple Mozilla products memory corruption/code injection/access restriction bypass vulnerabilities.** Multiple Mozilla products are prone to multiple vulnerabilities. These issues include various memory-corruption, code-injection, and access-restriction-bypass vulnerabilities. Other undisclosed issues may have also been addressed in the various updated vendor applications. Successful exploitation of these issues may permit an attacker to execute arbitrary code in the context of the affected application. This may facilitate a compromise of the affected computer; other attacks are also possible. For a complete list of vulnerable products: <http://www.securityfocus.com/bid/16476/info>
Solution: Please see the referenced vendor advisories for details on obtaining and applying fixes: <http://www.securityfocus.com/bid/16476/references>
Source: <http://www.securityfocus.com/bid/16476/discuss>
38. *August 21, Tech Web* — **Wikipedia "vandalism" entry vandalized.** The Wikipedia page on "vandalism" was vandalized Saturday, August 19, prompting the online encyclopedia to lock down the entry. Wikipedia has been forced to change some of its open-door, anyone-can-edit policies in the past because of misuse.
Source: <http://www.techweb.com/wire/security/192202407>
39. *August 21, eWeek* — **Microsoft dismisses PowerPoint zero-day warning.** Microsoft is dismissing a warning from anti-virus vendor Trend Micro that a new PowerPoint zero-day attack is under way. The Trend Micro warning, first issued Saturday, August 19, said that a specially crafted ".ppt" file was being used to exploit an undocumented PowerPoint vulnerability. The Japanese anti-virus company said it received a sample of the file August 17, less than two weeks after Microsoft shipped a security update to fix a PowerPoint flaw. However, according to Stephen Toulouse, a program manager in the Microsoft Security Response Center, the vulnerability has already been resolved by an update.
Source: <http://www.eweek.com/article2/0,1895,2006489,00.asp>
40. *August 21, CNET News* — **Kevin Mitnick Website hacked.** Instead of the usual description of Kevin Mitnick, his consulting services and books, the famed hacker's Website on Sunday, August 20, displayed a vulgar message. Online vandals, apparently operating from Pakistan, broke into the computer hosting Mitnick's Website on Sunday and replaced his front page with one of their own. As a result, four Web addresses belonging to Mitnick, including KevinMitnick.com and MitnickSecurity.com, displayed an explicit message on Mitnick and hacking. The attackers gained complete control over the server that hosts his site as well as others at hosting provider Hostedhere, Mitnick said. Website defacements still occur often, but they have become less high profile in recent years as other, financially motivated threats take the spotlight.
Screen shot: <http://www.zone-h.org/content/view/14073/31>
Source: <http://news.com.com/Kevin+Mitnick+Web+site+hacked/2100-7349>

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	1026 (win-rpc), 445 (microsoft-ds), 80 (www), 57715 (---), 62641 (---), 4672 (eMule), 135 (epmap), 139 (netbios-ssn), 54856 (---), 113 (auth) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/ .	

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

41. *August 22, New York Times* — **Britain charges 11 in plane case; bomb gear cited.** The British authorities charged 11 people on Monday, August 21, in connection with a suspected plot to blow up United States-bound airliners, and said investigators had discovered “martyrdom videos” and bomb-making materials in a far-reaching search of homes, cars, woodland, and other locations. Peter Clarke, the head of London’s anti-terrorism police said the police have found bomb-making chemicals, including hydrogen peroxide, and electrical components, recalling earlier British and American accounts that there was a plan to mix liquids into an explosive cocktail once they had been carried aboard airliners. The 11 charged, were arraigned Tuesday, August 22, and do not include all of those on a list issued earlier by the Bank of England of people whose assets were being frozen as part of the inquiry. The information disclosed Monday gave a sense of the scope of the investigation, beginning with months of surveillance of the suspects before most were arrested on August 10 that produced “highly significant video and audio recordings,” said Clarke.

Source: <http://www.nytimes.com/2006/08/22/world/europe/22britain.html?hp&ex=1156305600&en=5901695526c45409&ei=5094&partner=homepage>

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.